

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Russell N Owen, et al.

Application No.: 10/524,353

Filed: February 14, 2005


For: SYSTEM AND METHOD FOR SECURE CONTROL
OF RESOURCES OF WIRELESS MOBILE
COMMUNICATION DEVICES

§
§ Group Art Unit: 2435
§
§ Examiner: Darren B. Schwartz
§
§ Confirmation No.: 4652
§
§
§

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF EFS-WEB FILING

Pursuant to 37 C.F.R. §1.8, I hereby certify that this
correspondence is being electronically submitted to the U.S.
Patent and Trademark Office website, www.uspto.gov, on



Susan Caglagis

APPEAL BRIEF

Dear Sirs:

This Appeal Brief is filed in support of the appeal in the above-referenced application and is filed pursuant to the Notice of Appeal filed August 20, 2010. The Appellants authorize all required fees under 37 C.F.R. § 1.17 to be charged to Deposit Account No. 50-1515, of Conley Rose, P.C. of Texas.

TABLE OF CONTENTS

I.	Real Party in Interest	3
II.	Related Appeals and Interferences	3
III.	Status of Claims.....	3
A.	Total Number of Claims in the Application	3
B.	Status of All Claims in the Application.....	3
C.	Claims on Appeal	3
IV.	Status of Amendments.....	3
V.	Summary of the Claimed Subject Matter	4
VI.	Grounds for Rejection to be Reviewed on Appeal	7
VII.	Arguments.....	8
A.	To anticipate claims 1, 3-11, and 19-28, <i>Gbadegesin</i> must teach each and every element of independent claims 1, 11, and 26.....	8
B.	Even if <i>Gbadegesin's</i> virtual machines are interpreted as domains, <i>Gbadegesin</i> fails to anticipate claims 1, 3-11, and 19-28 because <i>Gbadegesin</i> fails to teach a first domain with a first level of trust and a second domain with a second level of trust, wherein the first level of trust only allows operations within the first domain.....	8
C.	<i>Gbadegesin</i> fails to anticipate claims 1, 3-10, 21-23, and 25 because <i>Gbadegesin</i> fails to teach a domain controller configured to determine whether the request originated from a first entity.....	11
D.	<i>Gbadegesin's</i> virtual machines are not domains	13
E.	Claim 2 is allowable because it depends from an allowable claim 1,	15
VIII.	Conclusion	16
IX.	Claims Appendix	17
X.	Evidence Appendix.....	24
XI.	Related Proceedings Appendix.....	25

I. REAL PARTY IN INTEREST

The real party in interest in the instant application is the following party: Research In Motion, Ltd.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

A. Total Number of Claims in the Application

Claims in the application: 1-28.

B. Status of All Claims in the Application

1. Claims canceled: 12-18.

2. Claims withdrawn from consideration but not canceled: None.

3. Claims pending: 1-11 and 19-28.

4. Claims allowed: None.

6. Claims objected to: None.

5. Claims rejected: 1-11 and 19-28.

C. Claims on Appeal

Claims on appeal: 1-11 and 19-28.

IV. STATUS OF AMENDMENTS

No substantive amendments were filed after the May 21, 2010 Final Office Action (hereinafter "Final Office Action"). However, prior to filing this Appeal Brief a Rule 41.33

Amendment was filed on January 20, 2011 to correct obvious typographical and minor errors in claims 7, 11, and 26.

Because the Rule 41.33 Amendment was filed after the filing of the Notice of Appeal, but prior to the date of filing this Appeal Brief, and because the amendments made in the Rule 41.33 Amendment were merely to present the rejected claims in better form for consideration on appeal, Appellants respectfully submit that the Rule 41.33 Amendment should be entered. *See* MPEP 1206(I). Additionally, because Appellants have not been notified of the non-entry of the Rule 41.33 Amendment and the reasons for non-entry, Appellants assume that the Rule 41.33 Amendment has been entered. *See id.*

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

This section provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number. Each element of the claims is identified with a corresponding reference to the specification where applicable. The citation to passages in the specification for each claim element does not imply that the limitations from the specification should be read into the corresponding claim element.

Handheld and other portable computers, such as wireless devices are frequently used for both business and personal needs. The wireless devices may be personally owned by users, or owned by a corporation. Regardless of who owns the wireless device, it may be likely to come into contact with corporate data such as contact lists, calendar entries, and email. The wireless device may be likely to come into contact with personal data outside of the corporation. In addition to the corporation and user, a wireless carrier will also have an interest in the device

regarding the wireless communications. Each stakeholder that has an interest in the wireless device may be in conflict with the interests of other stakeholders. For example, allowing a personal device access to the corporate network presents security risks. Also, the wireless carrier may have an interest in controlling the traffic flow to or from the device. The conflicting interests of the stakeholders may be protected by creating domains for each stakeholder.

The cited art, namely U.S. Patent Application Publication 2003/0065676 (*Gbadegesin*), discloses a method and system of managing concurrent access to multiple resources. Specifically, *Gbadegesin* creates resource sets within a computer and defines access control lists for the resource sets. Principals may access the resource sets based upon the access control lists. *Gbadegesin* defines principals as entities that may be given permission to perform certain operations. *Gbadegesin* also creates virtual machines on the computer, such that principals on one virtual machine may access resources on a second virtual machine.

The present application discloses a system and method for secure control of resources of wireless mobile communication devices. While the present system and method may include accessing resources, the resources are logically separated in domains, such that entities in a first domain may not access the resources of a second domain.

Claim 1 recites a wireless mobile communication device, *see, e.g.*, Application at p. 6, ll. 10-14, comprising: at least one memory storing a first domain, *see, e.g.*, Application at p. 6, l. 24 – p. 7, l. 16, comprising a first set of assets each sharing a first level of trust, *see, e.g.*, Application at p. 9, ll. 19-29, and the at least one memory storing a second domain comprising a second set of assets each sharing a second level of trust, wherein the first level of trust is different than the second level of trust; *see, e.g.*, Application at p. 11, ll. 22-31, and a domain controller configured to control the first domain and the second domain, and further configured

to control access to the first set of assets and the second set of assets; wherein the domain controller is further configured to receive a request to perform an operation affecting a particular asset in the first set of assets and to determine whether the request originated from a first entity that has a first trust relationship with the first domain, *see, e.g.*, Application at p. 24, l. 29 – p. 25, l. 20, and wherein the domain controller is further configured to permit completion of the operation affecting the particular asset only if the request originated from the first entity, and wherein the domain controller is further configured to permit the first entity to perform operations with respect to each of the first set of assets, *see, e.g.*, Application at p. 25, l. 21 – p. 26, l. 16.

Claim 11 recites a method for secure control of a wireless mobile communication device, *see, e.g.*, Application at p. 6, ll. 10-14, comprising segregating a plurality of assets of the wireless mobile communication device into a first set of assets in a first domain and into a second set of assets in a second domain, *see, e.g.*, Application at p. 9, ll. 19-29, wherein the first set of assets includes at least two different types of assets, wherein the first set of assets share a first level of trust to access, wherein the second set of assets share a second level of trust to access, and wherein the first level of trust is different than the second level of trust; *see, e.g.*, Application at p. 11, ll. 22-31, receiving a request from a first entity to perform an operation affecting at least one of the first set of assets; *see, e.g.*, Application at p. 24, l. 29 – p. 25, l. 20, determining, via a domain controller configured to control the first domain and the second domain, whether the operation is permitted by the first domain, wherein the operation is permitted by the first domain if the first entity has a first trust relationship with the first domain and further wherein the first entity is allowed to perform operations with respect to each of the first set of assets; and allowing

the operation to be completed only if the operation is permitted by the first domain, *see, e.g.*, Application at p. 25, l. 21 – p. 26, l. 16.

Claim 26 recites a computer readable medium storing program code, *see, e.g.*, Application at p. 33, ll. 7-18, which, when executed by a processor, performs a method for secure control of a wireless mobile communication device, *see, e.g.*, Application at p. 6, ll. 10-14, the method comprising: segregating a plurality of assets of the wireless mobile communication device into a first set of assets in a first domain and into a second set of assets in a second domain, *see, e.g.*, Application at p. 9, ll. 19-29, wherein the first set of assets includes at least two different types of assets, wherein the first set of assets share a first level of trust to access, wherein the second set of assets share a second level of trust to access, and wherein the first level of trust is different than the second level of trust; *see, e.g.*, Application at p. 11, ll. 22-31, receiving a request from a first entity to perform an operation affecting at least one of the first set of assets; *see, e.g.*, Application at p. 24, l. 29 – p. 25, l. 20, determining, via a domain controller configured to control the first domain and the second domain, whether the operation is permitted by the first domain, wherein the operation is permitted by the first domain if the first entity has a first trust relationship with the first domain and further wherein the first entity is allowed to perform operations with respect to each of the first set of assets; and allowing the operation to be completed only if the operation is permitted by the first domain, *see, e.g.*, Application at p. 25, l. 21 – p. 26, l. 16.

VI. GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1, 3-11, and 19-28 are anticipated under 35 U.S.C. § 102(b) by *Gbadegesin*.

2. Whether claim 2 is rendered obvious under 35 U.S.C. § 103(a) by *Gbadegesin* in view of U.S. Patent Application Publication 2003/0163685 (*Paatero*).

VII. ARGUMENTS

A. To anticipate claims 1, 3-11, and 19-28, *Gbadegesin* must teach each and every element of independent claims 1, 11, and 26.

Claims 1, 3-11, and 19-28 stand rejected under 35 U.S.C. § 102(b) as being anticipated by *Gbadegesin*. Claims 3-10, 21-23, and 25 depend from independent claim 1, claims 19, 20, and 24 depend from independent claim 1, and claims 27 and 28 depend from independent claim 26. Thus, claims 1, 3-11, and 19-28 stand or fall on the application of *Gbadegesin* to independent claims 1, 11, and 26. According to the Court of Appeals for the Federal Circuit, “[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros. v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The Appellant respectfully asserts that *Gbadegesin* fails to teach each and every element of independent claims 1, 11, and 26, and consequently fails to anticipate claims 1, 3-11, and 19-28.

B. Even if *Gbadegesin*’s virtual machines are interpreted as domains, *Gbadegesin* fails to anticipate claims 1, 3-11, and 19-28 because *Gbadegesin* fails to teach a first domain with a first level of trust and a second domain with a second level of trust, wherein the first level of trust only allows operations within the first domain

Gbadegesin fails to anticipate claims 1, 3-11, and 19-28 because *Gbadegesin* fails to teach a first domain comprising a first set of assets each sharing a first level of trust, and a second domain comprising a second set of assets each sharing a second level of trust, wherein the first level of trust only allows operations within the first domain. Claims 1, 11, and 26 read:

1. A wireless mobile communication device, comprising:

at least one memory storing a first domain comprising a first set of assets each sharing a first level of trust, and the at least one memory storing a second domain comprising a second set of assets each sharing a second level of trust, wherein the first level of trust is different than the second level of trust; and

a domain controller configured to control the first domain and the second domain, and further configured to control access to the first set of assets and the second set of assets;

wherein the domain controller is further configured to receive a request to perform an operation affecting a particular asset in the first set of assets and to determine whether the request originated from a first entity that has a first trust relationship with the first domain; and

wherein the domain controller is further configured to permit completion of the operation affecting the particular asset only if the request originated from the first entity, and wherein the domain controller is further configured to permit the first entity to perform operations with respect to each of the first set of assets.

11. A method for secure control of a wireless mobile communication device, comprising:

segregating a plurality of assets of the wireless mobile communication device into a first set of assets in a first domain and into a second set of assets in a second domain, wherein the first set of assets includes at least two different types of assets, wherein the first set of assets share a first level of trust to access, wherein the second set of assets share a second level of trust to access, and wherein the first level of trust is different than the second level of trust;

receiving a request from a first entity to perform an operation affecting at least one of the first set of assets;

determining, via a domain controller configured to control the first domain and the second domain, whether the operation is permitted by the first domain, wherein the operation is permitted by the first domain if the first entity has a first trust relationship with the first domain and further wherein the first entity is allowed to perform operations with respect to each of the first set of assets; and

allowing the operation to be completed only if the operation is permitted by the first domain.

26. A computer readable medium storing program code which, when executed by a processor, performs a method for secure control of a wireless mobile communication device, the method comprising:

segregating a plurality of assets of the wireless mobile communication device into a first set of assets in a first domain and into a second set of assets in a second domain, wherein the first set of assets includes at least two different types of assets, wherein the first set of assets share a first level of trust to access, wherein the second set of assets share a second level of trust to access, and wherein the first level of trust is different than the second level of trust;

receiving a request from a first entity to perform an operation affecting at least one of the first set of assets;

determining, via a domain controller configured to control the first domain and the second domain, whether the operation is permitted by the first domain, wherein the operation is permitted by the first domain if the first entity has a first trust relationship with the first domain and further wherein the first entity is allowed to perform operations with respect to each of the first set of assets; and allowing the operation to be completed only if the operation is permitted by the first domain.

(Emphasis added). As shown above, claims 1, 11, and 26 require a first domain comprising a first set of assets each sharing a first level of trust, and a second domain comprising a second set of assets each sharing a second level of trust, wherein the first level of trust only allows operations within the first domain. In contrast, *Gbadegesin's* computer comprises a plurality of virtual machines:

To practice the method illustrated with respect to FIG. 2, multiple virtual machines are launched as shown in FIG. 3. FIG. 3 illustrates components of a computer system employing one embodiment of the invention. In FIG. 3, a computer 300 originally comprises two resource sets, resource set A 340 and resource set B 360. The computer has two virtual machines, each of which is associated with one resource set. In particular, virtual machine A (VMA) 311 and virtual machine B (VMB) 312 are associated with resource set A 340 and resource set B 360, respectively. Unprivileged application A 321 and privileged application B 322 are assigned to VMA and are running on a desktop A 331 operated by VMA. A desktop represents a visual workspace that is accessed through a graphical user interface. Unprivileged application C 323 is assigned to VMB and is running on a desktop B 332 operated by VMB. Although the exemplary embodiment illustrated in FIG. 3 has a desktop for each of the virtual machines, this is not an absolute requirement. Other embodiments with a virtual machine lacking a desktop or having more than one desktop are not intended to be excluded by FIG. 3 from the scope of the invention described herein.

Gbadegesin, ¶ 29 (emphasis added). As shown above, *Gbadegesin's* computer system comprises a plurality of VMs. *Gbadegesin's*, VMs each comprise access control lists, applications, and principals. *Gbadegesin's* access control lists allow certain resources to be shared from one virtual machine to another:

Application instances are assigned to virtual machines, each of which is associated with a set of resources. Access control lists specify, for each principal, whether application instances owned by the principal can perform various resource-access operations. Specifically, an application instance is termed "unprivileged" if, by reason of its principal's permissions, it may never concurrently access resources in more than one virtual machine. A "privileged" application instance, on the other hand, may or may not be allowed such concurrent access, depending on circumstances such as the nature of the requested resources.

Gbadegesin, ¶ 22 (emphasis added). As shown above, *Gbadegesin*'s access control lists allow principals to communicate between VMs. As shown above in claims 1, 11, and 26, the first level of trust only allows operations in the first domain. If the VMs are the equivalent of domains as suggested by the Examiner, communication between the different VMs would not be allowed based on the features of claims 1, 11, and 26. However, *Gbadegesin*'s VMs communicate with each other. Therefore, *Gbadegesin* fails to teach a first domain comprising a first set of assets each sharing a first level of trust, and a second domain comprising a second set of assets each sharing a second level of trust, wherein the first level of trust only allows operations within the first domain. As such, *Gbadegesin* fails to teach each and every element of claims 1, 11, and 26 and consequently fails to anticipate claims 1, 3-11, and 19-28.

- C. *Gbadegesin* fails to anticipate claims 1, 3-10, 21-23, and 25 because *Gbadegesin* fails to teach a domain controller configured to determine whether the request originated from a first entity

Gbadegesin fails to anticipate claims 1, 3-10, 21-23, and 25 because *Gbadegesin* fails to teach a domain controller configured to determine whether the request originated from a first entity. Claim 1 reads:

1. A wireless mobile communication device, comprising:
at least one memory storing a first domain comprising a first set of assets each sharing a first level of trust, and the at least one memory storing a second

domain comprising a second set of assets each sharing a second level of trust, wherein the first level of trust is different than the second level of trust; and

a domain controller configured to control the first domain and the second domain, and further configured to control access to the first set of assets and the second set of assets;

wherein **the domain controller is further configured to receive a request to perform an operation affecting a particular asset in the first set of assets and to determine whether the request originated from a first entity** that has a first trust relationship with the first domain; and

wherein the domain controller is further configured to permit completion of the operation affecting the particular asset only if the request originated from the first entity, and wherein the domain controller is further configured to permit the first entity to perform operations with respect to each of the first set of assets.

(Emphasis added). As shown above, claim 1 requires a domain controller configured to determine whether a request originated from a first entity. In contrast, *Gbadegesin's* management facility compares permissions with access control lists:

The management facility 380 operates, in part, by comparing the permissions given to principals with various access control lists. An exemplary access control list A accompanying resource set A may specify: a) that applications run by users A, B, and C may access resource set A; b) that user A may access resources R1 and R2 in resource set A, user B may access resources R2 and R3, and user C may access resource R1; and c) that all three users may create new resources in resource set A. An exemplary access control list B accompanying resource set B may specify: a) that only users B and C may access resource set B; b) that users B and C may access all resources in resource set B; and c) that no user may create a resource in resource set B. In addition to the access control lists, the management facility also maintains a record of: a) assignment relationships between virtual machines and application instances; and b) association relationships between resource sets and virtual machines.

Gbadegesin, ¶ 33 (emphasis added). As shown above, *Gbadegesin's* management facility compares permissions given to principals with various access control lists. The Examiner incorrectly asserts that determining where a request originated from is the equivalent of comparing permissions. The meaning of the phrase, “determine whether the request originated from a first entity that has a first trust relationship with the first domain” is clear and unambiguous. The claimed phrase takes an active step. That active step is to **determine**

whether the request originated from a first entity that has a first trust relationship with the first domain. This claimed feature is not the same as “comparing permissions” as in *Gbadegesin*. For example, one could check to see if a principal has permission to access a resource without actually determining whether the request actually originated from that principal. Making the determination as to origin would be an additional step.

The Examiner asserts that, “One of ordinary skill would conquer [*sic*] that if a principal has permission to access a resource, such a request to access said resource must have ‘originated’ from an approved source.” *Advisory Action*, p. 2. The Examiner’s assertion is incorrect. As a non-limiting example, a request might appear to be from a principal (such as having a forged return address) but not actually be from the principal. Furthermore, one may check to see if a principle has permission to access a resource without actually determining whether the request originated form the principal. Checking for permission, as asserted to be shown in *Gbadegesin*, and determining the origin of the request, as in claim 1, are clearly different. Therefore, *Gbadegesin* fails to teach a domain controller configured to determine whether the request originated from a first entity. As such, *Gbadegesin* fails to teach each and every element of claim 1 and consequently fails to anticipate claims 1, 3-10, 21-23, and 25.

D. *Gbadegesin*’s virtual machines are not domains

The Examiner asserts that *Gbadegesin*’s virtual machines (VMs) are the equivalent of the domains of claims 1, 11, and 26. *See* Office Action dated May 21, 2010 (*Office Action*), pp. 3 & 5. The Examiner admits that *Gbadegesin* fails to define virtual machine. *See* *Advisory Action* dated July 23, 2010 (*Advisory Action*), p. 2. The ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at

the time of the invention, i.e., as of the effective filing date of the invention. MPEP § 2111.01(III). Newton's Telecom Dictionary 22nd Edition defines VM as part of a computer's hard disk that thinks it is another computer. Newton's goes on to say the VM thinks it is a complete computer and doesn't know about the "real" computer except in terms of what the software creating the VM chooses to share with it. Thus, a VM is software that mimics the performance of a hardware device. VMs may emulate an entire system platform to include execution of an operating system (OS). Multiple VMs typically share an underlying physical resource. However, each VM behaves as if it is running on the physical resource alone. VMs allow multiple copies of an OS to run on a single physical resource. It is noted that the VM itself may be programmed to tell the software running on it that other VMs exist. However, each VM functions as a separate physical machine, even though a plurality of VMs may be operating on a single physical resource.

The Examiner chooses to define domain as "a collection of objects that share a common level of trust, and can be owned and controlled by a mobile device stakeholder, such as a mobile device user, a mobile device owner, a carrier or a service provider." *Advisory Action*, p. 2. Based on what one of ordinary skill in the art would know of a virtual machine, and the definition of domain chosen by the Examiner, it is obvious that the claimed domains are not virtual machines as suggested by the Examiner. Furthermore, the claimed domains all function on a wireless device. A wireless device typically runs one instance of an operating system, and the claimed domains would all function under one single instance of that operating system. The VMs as defined each run their own instance of an operating system and function as if they were independent operating systems. Therefore, *Gbadegesin's* VMs could not possibly be the equivalent of the claimed domains.

E. Claim 2 is allowable because it depends from an allowable claim 1.

Claim 2 is allowable because it depends from an allowable claim 1. Claim 2 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Gbadegesin* in view of *Paatero*. Claim 2 depends from independent claim 1, which is allowable for the reasons given above. Thus, claim 2 is also allowable.

VIII. CONCLUSION


In view of the above arguments, the Appellants respectfully request that the final rejection of the claims be reversed and the case advanced to issue. If a telephone interview would advance prosecution of the instant application, then the Appellants invite the Examiner to call the attorneys of record.

The Commissioner is hereby authorized to charge payment of any further fees associated with any of the foregoing papers submitted herewith, or to credit any overpayment thereof, to Deposit Account No. 50-1515, of Conley Rose, P.C. of Texas.

Date: 1-20-11

5601 Granite Parkway, Suite 750
Plano, Texas 75024
Telephone: (972) 731-2288
Facsimile: (972) 731-2289

Respectfully submitted,
CONLEY ROSE, P.C.



J. Robert Brown, Jr.
Reg. No. 45,438

ATTORNEY FOR APPELLANTS

IX. CLAIMS APPENDIX

The text of the claims involved in the appeal is:

1. (Previously Presented) A wireless mobile communication device, comprising:
at least one memory storing a first domain comprising a first set of assets each sharing a first level of trust, and the at least one memory storing a second domain comprising a second set of assets each sharing a second level of trust, wherein the first level of trust is different than the second level of trust; and
a domain controller configured to control the first domain and the second domain, and further configured to control access to the first set of assets and the second set of assets;
wherein the domain controller is further configured to receive a request to perform an operation affecting a particular asset in the first set of assets and to determine whether the request originated from a first entity that has a first trust relationship with the first domain; and
wherein the domain controller is further configured to permit completion of the operation affecting the particular asset only if the request originated from the first entity, and wherein the domain controller is further configured to permit the first entity to perform operations with respect to each of the first set of assets.
2. (Previously Presented) The wireless mobile communication device of claim 1, further comprising a key store for storing cryptographic keys associated with the first domain, wherein the domain controller is configured to determine whether the first entity is using the cryptographic keys.

3. (Previously Presented) The wireless mobile communication device of claim 1, wherein the domain controller is configured to determine whether the first domain also includes the first entity.

4. (Previously Presented) The wireless mobile communication device of claim 1, wherein the first domain further includes as an asset a software application for which the domain controller permits completion of the operation upon the software application;

wherein completion of the operation is not permitted if the request originated with a second entity that does not have a trust relationship with the first domain.

5. (Previously Presented) The wireless mobile communication device of claim 4, wherein the wireless mobile communication device further comprises a super user software application that has a trust relationship with both the first domain and the second domain.

6. (Previously Presented) The wireless mobile communication device of claim 5, wherein both the first domain and the second domain include the super user software application.

7. (Previously Presented) The wireless mobile communication device of claim 1, wherein the domain controller is further configured to receive information, and to place the information into at least one of the first domain or the second domain.

8. (Previously Presented) The wireless mobile communication device of claim 1, wherein the first set of assets are selected from the group consisting of:

communication pipes, persistent data, properties, and software applications.

9. (Previously Presented) The wireless mobile communication device of claim 1, further comprising a data store for storing properties, wherein the domain controller is further configured to determine whether the operation is permitted by properties in the data store, and to permit completion of the operation if the operation is permitted by the properties in the data store;

wherein completion of the operation is not permitted if the operation is not permitted by the properties in the data store.

10. (Previously Presented) The wireless mobile communication device of claim 9, wherein each property is global, domain-specific, or specific to a particular software application on the wireless mobile communication device.

11. (Previously Presented) A method for secure control of a wireless mobile communication device, comprising:

segregating a plurality of assets of the wireless mobile communication device into a first set of assets in a first domain and into a second set of assets in a second domain, wherein the first set of assets includes at least two different types of assets, wherein the first set of assets share a first level of trust to access, wherein the second set of assets share a second level of trust to access, and wherein the first level of trust is different than the second level of trust;

receiving a request from a first entity to perform an operation affecting at least one of the first set of assets;

determining, via a domain controller configured to control the first domain and the second domain, whether the operation is permitted by the first domain, wherein the operation is permitted by the first domain if the first entity has a first trust relationship with the first domain and further wherein the first entity is allowed to perform operations with respect to each of the first set of assets; and

allowing the operation to be completed only if the operation is permitted by the first domain.

12-18. (Canceled)

19. (Previously Presented) The method of claim 11, further comprising the step of:

determining whether the operation is permitted by a property stored at the wireless mobile communication device,

wherein the step of allowing comprises the step of allowing the operation to be completed if the operation is permitted by both the first domain and the property;

wherein the operation is not allowed to be completed if the operation is not permitted by both the first domain and the property, and

wherein the step of determining whether the operation is permitted by the property comprises checking a global property for the wireless mobile communication device and a domain property for the first domain.

20. (Previously Presented) The method of claim 19, wherein the request originates from a software application, and wherein the step of determining whether the operation is permitted further comprises checking an application property for the software application.
21. (Previously Presented) The system of claim 1, wherein the first set of assets includes at least two different assets selected from the group consisting of: communication pipes, persistent data, properties, and software applications.
22. (Previously Presented) The wireless mobile communications device of claim 1 wherein the domain controller is further configured to deny completion of the operation of the particular asset if the request originated from a second entity that does not have the first trust relationship with the first domain.
23. (Previously Presented) The wireless mobile communications device of claim 22 wherein the second entity has a second trust relationship with the second domain, and wherein the domain controller is further configured to permit the second entity to perform operations with respect to each of the second set of assets.
24. (Previously Presented) The method of claim 11 further comprising:
denying completion of the operation if the request originated from a second entity that does not have the first trust relationship with the first domain.

25. (Previously Presented) The method of claim 22 wherein the second entity has a second trust relationship with the second domain, and wherein the method further comprises:

permitting the second entity to perform operations with respect to each of the second set of assets.

26. (Previously Presented) A computer readable medium storing program code which, when executed by a processor, performs a method for secure control of a wireless mobile communication device, the method comprising:

segregating a plurality of assets of the wireless mobile communication device into a first set of assets in a first domain and into a second set of assets in a second domain, wherein the first set of assets includes at least two different types of assets, wherein the first set of assets share a first level of trust to access, wherein the second set of assets share a second level of trust to access, and wherein the first level of trust is different than the second level of trust;

receiving a request from a first entity to perform an operation affecting at least one of the first set of assets;

determining, via a domain controller configured to control the first domain and the second domain, whether the operation is permitted by the first domain, wherein the operation is permitted by the first domain if the first entity has a first trust relationship with the first domain and further wherein the first entity is allowed to perform operations with respect to each of the first set of assets; and

allowing the operation to be completed only if the operation is permitted by the first domain.

27. (Previously Presented) The computer readable medium of claim 26, wherein the method performed by the executed program code further comprises:

denying completion of the operation if the request originated from a second entity that does not have the first trust relationship with the first domain.

28. (Previously Presented) The computer readable medium of claim 27 wherein the second entity has a second trust relationship with the second domain, and wherein the method performed by the executed program code further comprises:

permitting the second entity to perform operations with respect to each of the second set of assets.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.